Provided for Public Comment: October 16,1996

Governor's Work Group on Commercial Access to Government Electronic Records

DRAFT POSITION PAPER ON QUESTION 2

The second of three position papers prepared for the consideration of the Work Group

SAFEGUARDING PERSONAL INFORMATION

How can citizens be assured that personal information about them will be safeguarded when public records in electronic format are released for business or commercial purposes?

I. The Privacy Landscape

The digitization of records containing personally identifiable information has compounded some long-standing privacy concerns and, in some cases, created new ones. Since the Governor announced the creation of this Work Group on March 30, 1996, there have been dozens of news stories about the impact of digital technology on the use and abuse of personally identifiable information.

It is instructive to review the developments concerning privacy and technology during the Work Group's brief tenure. These stories are illustrative of the revelations that are fueling concern among citizens and with which public policy makers must deal:

- **TAPE RECORDING CALLS:** The Washington State Patrol has suspended what had become a routine practice of recording private telephone conversations made from certain rooms at its Parkland, WA headquarters. According to published reports State Patrol Captain John Baptiste said the digital recordings constituted a "a technical violation that did no harm." He said it was an innocent error made in the interest of improving efficiency. Calls were recorded for over a year without any notice telling callers their phone conversations were being recorded.[1] The Washington State Privacy Act restricts the recording of private conversations, making it unlawful to make recordings without first obtaining the consent of all parties to the communication.

[1] John Gillis, "State Patrol admits it violated law," *Tacoma News Tribune*, Friday, October 18, 1996: A1, A10.

- **PERSONAL USE OF AIDS/HIV DATABASE:** A computer database of nearly 4,000 AIDS and HIV infected individuals was allegedly used by a Florida man to look up the names of potential dates for himself and his friends. Called "the nation's largest ever security breach of AIDS information," the case "has thrown a spotlight on new threats to medical confidentiality as computer networks, insurance databases and hackers pry out the most intimate details of people's lives." Copies of the list of individuals were sent to the man's employer -- the state department of health -- and two area newspapers. Officialsare investigating whether the list may have been published on the Internet or whether there is a network of AIDS information brokers.[2]

- **SURF TRACKING:** The 1996 Equifax/Harris Consumer Privacy Survey for the Internet illustrated the changes in perceptions that come with using a new technology. Seventy-one percent of Internet users believed the tracking of their activities on the Internet was intrusive, compared to sixty-three percent of non-users. Sixty percent of users said their anonymity should not be compromised when they visit a Web site or use e-mail. Only 45 percent of non-users "were sympathetic to the desire for online anonymity."[3]

- **INTERNET PRIVACY PROTECTION:** An Internet Privacy protection bill has been introduced in Congress, the latest in a series of legislative measures at the federal level to slow the flow of personally identifiable information.[4] Key provisions of the proposed federal Health Information Privacy Protection Act are intended to curb the growing trade in medical records.[5] Other initiatives included proposed regulations for the use of so-called smart cards over networks[6] and the introduction of (hotly contested) encryption standards.[7] In addition, the Attorney General has proposed new measures to prevent acts of online terrorism.[8]

- **E-MAIL, VOICE MAIL AND PERSONAL AGENTS:** The proliferation of e-mail and voice mail in the private sector has raised concerns over employer liability and personal privacy.[9] Recent anecdotal reports are often cast against the backdrop of a 1993 study published by *MacWorld* magazine. It found that thirty percent of

---

[2] "Aids list breach highlights confidentiality issues," *Reuters*, October 13, 1996.

[3] *BNA Daily Report for Executives*, October 10, 1996: A24.

[4] "Internet Privacy rules proposed," *Telecommunications Alert*, June 5, 1996, Vol. 13, No. 109.

[5] "Prepared statement by Steven Kenny Hoge M.D., Division of Government Relations, American Psychiatric Association, on the Health Information Privacy Protection Act [Discussion Draft] before the House Government Reform and Oversight Committee Subcommittee on Government Management, Information and Technology," *Federal News Service*, June 14, 1996.

[6] "Wait on smart card regulation, FDIC told," *The Regulatory Compliance Watch*, September 23, 1996,

[7] *Software Law Bulletin*, May, 1996: 77.

[8] Art Kramer, "Attorney General hopes to thwart online terrorists," *Atlanta Journal and Constitution*, June 6, 1996.

[9] "E-Mail and Voice Mail: Liability waiting to happen?" *Idaho Employment Law Letter*, July 1996, Volume 1, Issue 4; Robert Gellman, "On Privacy: The Question Industry doesn't want to answer," *DM News*, June 17, 1996: 44; and "Insurers, Corporations uncertain about need for on-line coverage," *Treasury Manager's Report*, August 30, 1996, No. 18, Vol. 4.

employers in the survey were searching the computer files kept by employees, leading to increased reports of boredom, tension, anxiety, depression, anger and fatigue. The introduction of personalized search agents on the Internet, which track the on-line habits of individuals to identify their interests, raises the prospect that the cache gathered about individuals might be used (and abused) by others.[10] To address the privacy concerns raised by this technology, electronic agent services have turned to independent auditors to ensure personally identifiable information is not intercepted or released to third parties.[11]

- **LEXIS-NEXIS P-TRACK CONTROVERSY:** The respected information research service and reseller Lexis-Nexis was the focus of a national controversy soon after it launched a new service called the P-TRACK Personal Locator file in June. The company's promotional material initially said the service "provides up to three addresses, as well as aliases, maiden names, and Social Security numbers" of "300 million names right at your fingertips." Fueled by media coverage and Internet message traffic, Lexis-Nexis was flooded with complaints about the potential for fraud or other abuse.[12] Eleven days after P-TRACK launched, Lexis-Nexis removed the Social Security numbers from the service and provided a mechanism for removing names from the data base upon request.[13] In its defense, a company spokesperson said, "There are a lot of people that don't understand how information is collected by any number of agencies. We are not the only company that purchases this type of database."[14]

- **FTC SAFEGUARDS:** In response to the complaints over P-TRACK, the Federal Trade Commission (FTC) urged Congress to tighten controls on commercial services that provide personally identifiable information about individuals for a fee.[15]

- **INDUSTRY PRIVACY PRINCIPLES FOR THE INTERNET:** A consortium of companies involved in electronic commerce via the Internet announced plans to develop a set of privacy principles for doing business over the global network. The Privacy Assured group came together in the wake of the Lexis-Nexis P-Track controversy. According to published reports, "Privacy Assured, which is a pilot program of the Electronic Frontier Foundation's eTrust project, will post its blue PA logo on Web sites that adhere to its standards". The proposed standards would prohibit member companies from knowingly listing information about individuals that

---

[10] "An intelligent agent is simply a computer program endowed with enough smarts to act as your personal assistant. In theory, an intelligent agent can act as your secretary, reference librarian, or stockbroker. It's designed to roam the Internet in search of just the information, sounds, or pictures you want. " See "Agents work for you," NetGuide Magazine, July 1, 1996.

[11] Rose Aguilar, "Privacy audit can keep secret," *Reuters*, August 6, 1996, 1:30 p.m. PT

[12] Tom Abate and Erin McCormick, "When technology threatens privacy: Public anger grows as data providers sell our names, numbers and address," *The San Francisco Examiner*, September 20, 1996: A1.

[13] Thomas E. Weber, "Lexis-Nexis Database Sparks Outcry on the Internet about Privacy Issues," *Wall Street Journal*, Sept. 19, 1996.

[14] Janet Kornblum, "Private lives online," *c|net news.com*, October 11, 4 p.m. PT

[15] "FTC comes along on privacy," *Reuters*, September 23, 1996, 6:45 p.m. PT

has not been volunteered for publication. The eTrust program would disallow reverse searches to determine individuals' names from e-mail addresses, phone numbers or other information. Companies adhering to the standard would only release aggregated usage statistics, not individual information; and give individuals the option to remove their personal information from lists.[16]

- **"KIDS OFF LISTS" PROVISIONS:** The federal Children's Privacy Protection and Parental Empowerment Act put in place restrictions on online solicitation of children with a view to keep information about them out of the hands of sexual predators.[17] As part of a conference on Internet privacy, the FTC examined online marketing to children -- including the collection and sale of information about their online behavior.[18] The Direct Marketing Association responded with a preliminary set of privacy guidelines for self-regulation. The proposal, if approved, would require marketers to post a privacy policy in an "easy-to-find, easy-to-read statement" that tells users how the information will be used.[19]

- **QUESTIONABLE DATA USE AND INTEGRITY:** A long-time information re-seller is reconsidering its business model following a controversy over the use of automated mail information by a subsidiary.[20] Other recent stories have focused on data integrity and concerns about the accuracy of credit information. Some of these stories use as their benchmark a 1991 review of personally identifiable information held by the major national credit reporting agencies. It found errors in 48 percent of records checked in 1991, an increase of 5 percent since a similar review in 1988.

- **OREGON DMV RECORDS ON THE 'NET:** Oregon Governor John Kitzhaber will ask the 1997 legislature to redress the balance between privacy and public disclosure in the wake of a controversy over the publishing of the state's DMV records on the Internet. A Portland-based computer enthusiast, Aaron Nabil, purchased the Oregon DMV database for $222 and posted it on the World Wide Web.[21] The controversial Web site was suspended after Nabil and the state Department of Transportation were inundated with complaints from angry drivers "who mistakenly thought the records were private."[22]

---

[16] *Broadcasting & Cable*, October 7, 1996: 87.

[17] "Prepared Testimony of Marc Rotenberg, Director, Electronic Privacy Information Center before the House Committee on the Judiciary Subcommittee on Crime on the Children's Privacy Protection and Parental Empowerment Act, H.R. 3508," *Federal News Service*, September 12, 1996.

[18] Denise Shelton, "Children-targeted marketing under fire," *c|net news.com*, May 14, 1996, 2 p.m. PT

[19] Jim Davis, "Rules issued for online privacy," *c|net news.com*, June 4, 1996, 1 p.m. PT

[20] Nancy Millman, "Questionable data sale to hinder Metromail IPO? R.R. Donnelley says unit no longer fits in," *Chicago Tribune*, June 4, 1996: 1.

[21] William McCall, "Vehicle files on Internet draws anger," *Tacoma News Tribune*, Aug. 8, 1996. The Oregon case is not, strictly speaking, an example of commercial use because the provider is not charging for access. There are other such services -- such as Internet DMV -- that provides on line searching of a number of state databases for $20 to $35 per search.

[22] Anthony Lazarus and Mike Ricciuti, "DMV data drives protest," *Reuters*, August 8, 1996, 11:45 PT.

- **PRIVACY CONCERNS OVER ONLINE REGISTRIES:** Advances in networked computing lend themselves to the automation of routine information handling. Recently, there has been a proliferation of new online registries -- online voter registries,[23] an online motor vehicles registry,[24] an online workers compensation registry and an online drug registry.[25] The Social Security Administration is planning a pilot program to provide sensitive personal earnings information online.[26] The Internal Revenue Service (IRS) has suspended the development of Cyberfile, a service that would allow taxpayers to file their tax returns via the Internet, after a critical report that concluded the software used in the project was "undisciplined" and lacked adequate security requirements.[27] For its part, the U.S. State Department is distributing passport forms online but will not accept online registrations until network security and other technical issues are overcome.[28] Security concerns raised by these new registries and services parallel some of the perils of online shopping[29] and have also been linked to fears about e-mail disclosure.[30] Some of the new applications, which are collecting large amounts of personally identifiable information, have also brought with them concerns about how new sources of data will be used.[31]

- **FBI "FILEGATE" AND CREDIT STING:** There have been allegations of abuse of personally identifiable information by public officials, calling into question the trustworthiness of the public caretakers in these cases. In August, credit card holders reacted angrily when they learned that federal law enforcement officials had used their credit information without their consent as bait in a sting operation.[32] News of the sting came on the heels of the revelation that White House staff allegedly accessed the FBI files of hundreds of citizens who worked for the prior administration.[33]

- **DISCLOSING PERSONAL INFORMATION FOR THE PUBLIC GOOD:** There are cases when disclosing personally identifiable information may result in public benefit but the criteria for release varies widely. For example, the Health Professions Quality Assurance Division at the Washington State Department of Health regulates the practice of health professions and enforces health and safety laws that protect the public from negligent, incompetent, or illegal health care practices. The names and

---

[23] "Voters' register mustn't be an invasion of privacy," The Financial Post, August 22, 1996: 10, and

[24] Janet Kornblum, "Web has fast lane to DMV," *Reuters*, August 6, 1996, 5:30 p.m. PT

[25] John Deverell, "Drug registry sparks fears for privacy: Few rules yet on how new cache of data may be used," *The Toronto Star*, September 17, 1996: B1.

[26] Janet Kornblum, "Social Security sends info online," *Reuters*, September 27, 1996, 12:30 p.m., PT

[27] Rose Angular, "IRS back to drawing board," *Reuters*, August 30, 1996, 1 p.m. PT

[28] Janet Kornblum, "Your pass overseas, now online," *Reuters*, September 19, 1996, 1 p.m.

[29] Ilene Knable Gotts and Rebecca R. Fry, "Danger may await Internet shoppers," *The National Law Journal*, March 25, 1996: C9.

[30] Jim Dillon, "Digital Dialogue: Lexis-Nexis incident reveals e-mail disclosure fears," *The Dayton Daily News*, September 23, 1996: 15.

[31]

[32] Jim Newton, "Credit-card holders cry foul that accounts used in sting," *The Seattle Times*, Aug. 30, 1996.

[33] Howard M. Shapiro, "Prepared Report of the FBI General Counsel on the Dissemination of FBI File information to the White House," *Federal News Service*, June 14, 1996.

registration numbers of those health care professionals facing disciplinary action are published as a news release and posted on the Internet.[34]

- **PRIVACY RIGHTS OF CONVICTED CRIMINALS:** By contrast, the privacy rights of a convicted murderer and a convicted sex offender were upheld despite challenges by *The Seattle Times*. "Privacy is a hot-button word, one that people -- even criminals -- increasingly cite in wanting to control what is known about them..." wrote Times executive editor Michael R. Fancher in arguing that "the public has a higher right to information about such people and about how are institutions treat them."[35]

One commentator wrote of the fundamental change in the way electronic information is collected, manipulated and distributed, "Everything from our taxes, health care, work, travel and military records to past scrapes with police or even sexual escapades -- somewhere the information is only a few keystrokes away. The possibility for abuse is breathtakingly large -- and growing."[36] The public response has been swift, sure, sometimes fearful, and sometimes angry. That citizen focus is vitally important in considering commercial access in general -- and the privacy question in particular.

II. Public Concern over Privacy in the Digital Age.

Over time, as some have argued, the cumulative effect of such stories and the seemingly relentless advance of technology may lower expectations of privacy. In the near term, however, the opposite appears to be the case. Many of the developments described above have been met with mounting public concern. Individuals have reacted quickly and vehemently to revelations that what they had assumed was private information was available publicly from a growing number of sources.

Writers told the Work Group that government has greater access to information about people's lives than do private-sector interests. Government collects personal information on license applications, entitlements, hunting licenses and the like. Citizens are required to provide personally identifiable information as a precondition of receiving some services or benefits from government. Government is trusted with personal information and the writers' expectations are that personally identifiable information would be handled in a way that would not break that trust. One writer expressed it this way: "The citizenry of the great state of Washington highly values its trust and confidence in its public servants ... to properly and adequately protect the individual, personal, and private interest and safety, in all functions of society."

The Work Group respects the concerns expressed through the many thoughtful comments it received from members of the public on this important question. In fact, the

---

[34] See the relevant page on the DOH web site at http://www.doh.wa.gov/Publicat/96-78.html

[35] Michael R. Fancher, "Two criminals' privacy protected by state courts -- and the public loses," *The Seattle Times*, Sunday, October 13, 1996: A27.

[36] David Gergen, "Our most valued right," *U.S. News & World Report*, June 24, 1996: 72.

overwhelming majority of comments from private citizens were concerned with privacy. In response to the revelations about the availability of personally identifiable information, writers called for additional protections on privacy. Some writers suggested that any privacy standards should be based on consent. Importantly, they wanted both to curb the amount of personally identifiable information in circulation in a networked world and to be notified that information about them was being gathered in the first place.

A number of writers expressed the fear that they could become victims of crime through the misuse of personally identifiable information. They expressed concerns about the prospect of credit or identity fraud and the risk of employment and insurance discrimination. The concerns extended to fear that personally identifiable information might be misused in cases of stalking and domestic violence. As one writer put it, "the simple fact is that there are a lot of us out here hiding from someone who wishes to do us harm."

In the view of many writers, computerization and digitization has brought with it the need for more safeguards and the need to "fight harder" to protect personally identifiable information. Some writers cited what they viewed as a lack of enforcement of existing laws and a lack of recourse in the case of violations. Still other writers questioned the necessity for the disclosure of personally identifiable information from government sources for secondary purposes, suggesting that there are alternative sources of information through consumer tracking and other private-sector initiatives.

Taken as a whole, public comment has tended to revolve around three policy and process questions:

- Who owns the unique copy of the record to which all others refer?
- What safeguards are in place to protect the integrity of the unique copy?
- What are the government's responsibilities related to secondary use of public records?

The majority report from the public is that there is an imbalance between technological advances and existing privacy protections.

III. Legislative Background.

Public policy on privacy "seeks to balance business' and government's needs for access to information with the individual's expectations of privacy."[37] In the veto messages that created the Work Group, the Governor recognized that its deliberations "will bring into focus a complicated debate that will reveal conflicting values about public records, privacy, the future of technology, and government accountability."[38] Efforts to

[37] David W. Danner and Phil Moeller, *Telecommunications in Transition: Fasciliating Advanced Communications Infrastructure in Washington*, Staff Report of the Washington State Senate Energy and Utilities Committee (February 1994).
[38] HB 2790 (Full Veto)

balance these competing values have resulted in both state legislation and citizen initiatives -- the Open Records Act and the Privacy Act being the most prominent among them.

The Washington State Privacy Act prohibits intercepting or recording of communications by phone, telegraph, radio, "or other devise" between two or more people without consent.[39] There are also statutory prohibitions on automatic dialing and announcing devices for solicitation purposes[40] and unsolicited fax messages.[41] In vetoing amendments to the Act in 1996, the Governor wrote that "Citizens' right to be secure in their private affairs and in their homes is essential to a free society. Washington State is very protective of people's right to privacy against governmental intrusions. The state constitution and Washington's Privacy Act afford greater protections that the federal Constitution and privacy laws...."[42]

For its part, the Open Records Act -- passed by a citizen initiative in 1971 -- provides broad access to government records to ensure the public's right to monitor government activities. "The people, in delegating authority, do not give their public servants the right to decide what is good for the people to know and what is not good for them to know. The people insist on remaining informed so that they may maintain control over the instruments that they have created."[43]

The Open Records Act also provides that "[t]his law shall not be construed as giving authority to any agency to give, sell or provide access to lists of individuals requested for commercial purposes, and agencies shall not do so unless specifically authorized or directed by law."[44] The Open Records Act also prohibits access to information "that is highly offensive to a reasonable person and of no legitimate public concern."[45]

In testimony before the Work Group, Dr. Ann Cavoukian[46], author of the book *Who Knows: Safeguarding Your Privacy in a Networked World*, situated the Washington Open Record's Act in the larger context of access and privacy legislation around the United States and internationally.

Dr. Cavoukian discussed what a public record is -- and what it means when public records contain personally identifiable information. She said that there is the need for greater definitional clarity between public records and those records that contain personally-identifiable information. She also provided an overview of Fair Information

---

[39] RCW 9.73.030
[40] RCW 80.36.400
[41] RCW 80.36.540
[42] ESHB 2406 (Full Veto)
[43] RCW 42.17.251
[44] Initiative 276, Section 25 (5)
[45] RCW 42.17.255
[46] Dr. Cavoukian is also the Assistant Commissioner of the Information and Privacy Commission of Ontario, Canada.

Practices code which, she noted, were originated by the United States in 1973.[47] The code emphasizes the 'use limitation principle' which provides that information should be used only for those purposes or reasons for which it was collected. The federal Freedom of Information Act (FOIA) and Washington state privacy law are based on this principle.

Dr. Cavoukian expressed concern that the provision in Washington's Open Records Act to prohibit access to information "that is highly offensive to a reasonable person and of no legitimate public concern" is a very high threshold and may be "too high" if there is to be meaningful protection of personal privacy. When in doubt, agencies are most likely to err on the side of releasing information. Dr. Cavoukian asked the Work Group to consider the merits of a countervailing privacy provision that would require greater care in the decision to release personally identifiable information.

The Work Group has also heard from other parties that have made the argument that any such suggestion is "misguided." Michael J. Killeen is with the Communications and Media Law Department of the law firm of Davis Wright Tremaine in Seattle and legal counsel to *The Seattle Times*.[48] In a submission to the Work Group, Mr. Killeen wrote,

> Policy makers should recognize the risks in denying access based on overly broad concerns about personal privacy -- risks that include loss of government accountability, an increased likelihood that official abuse will go undetected, less effective detection of dangers to public health or safety, and increased alienation of citizens from their government. The guiding presumption must be that if government has a reason to collect information about an individual, that information generally has an impact on the community, and therefore citizens are entitled to it.[49]

Mr. Killeen further wrote that "[p]olicies aimed at preventing misuse of public information should be formulated narrowly, in a way that does not unduly restrict access." In a story not directly related to the Work Group's activities, Seattle Times executive editor Michael R. Fancher recently told readers, "The Times has no interest in invading the private lives

---

[47] Two summaries of Fair Information Practices are included as Appendices A and B. Appendix A reflects the work of the Organization for Economic Cooperation and Development (OECD) in Europe. Appendix B is the Canadian Standards Association (CSA) Draft Model Code for the Protection of Personal Information, which is adapted from the OECD principles to address concerns raised by the rise of electronic records.

[48] In his charge to the group, the Governor wrote, "the work group will not consider media access to government records in electronic format as a commercial use when such access is being requested for reporting purposes."

[49] Michael J. Killeen, "Electronic Records, the Public Disclosure Act, and Principles Governing Access," Presentation to the Governor's Work Group on Commercial Access to Electronic Records, July 11, 1996.

of ordinary citizens. Our interest in maintaining the public's access to information about the performance of public institutions or about public policy.[50]"

There may be common ground on this point. The Work Group has no interest in restricting access to information about the performance of public institutions or about public policy. The Work Group's interest is the government's duty to safeguard the private lives of ordinary citizens from invasion.

The Work Group notes with interest that the American Civil Liberties Union (ACLU) of Washington has begun an eighteen-month process to develop policies on commercial access to government records. In testimony before the group, ACLU-W Legislative Director Jerry Sheehan spoke of the organization's conflict on the issues related to commercial access. The ACLU has historically been a strong advocate of both access to government information and privacy. The present case is causing the organization to assess the two values in juxtaposition with a view to striking a balance between what appear to be competing interests.

That said, Dr. Cavoukian and other privacy advocates argue that openness in government and privacy protections for the individual are not competing but, rather, fundamentally compatible. She writes,

> [O]n one hand, the goal is to open the door and give people access to information, while on the other, the goal is to close the door and prevent outsiders from getting your information. But these two goals are seldom in conflict, for they apply to two entirely different types of information -- one public, one not. Freedom of information applies to the public records of the government, records that are generally *nonpersonal* -- that is, not about specific individuals. Privacy protection applies to a different set of records -- *personal information*, associated with specific individuals. Public records *should* be accessible to the public; private records *should* be kept private, and used only for the purpose for which they were obtained.[51]

The director of the Washington, D.C.-based Electronic Privacy Information Center, Marc Rotenberg, adds, "That there may be overlap between the public and the private does not diminish the essential importance of these principles.[52]"

IV. Privacy: A Right in the Balance.

---

[50] Michael R. Fancher, "Two criminals' privacy protected by state courts -- and the public loses," *The Seattle Times*, Sunday, October 13, 1996: A27.

[51] Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding your privacy in a networked world*, New York: McGraw-Hill, 1996: 40-41 *(Emphasis in the original)*

[52] Marc Rotenberg, "Privacy Protection," *Government Information Quarterly* Vol. 11, No. 3, 1994: 254.

The intersection of access and privacy is made even more difficult to navigate in the present case by rapid technological change and a historic problem with defining the concept of privacy

In 1928, Justice Louis Brandeis called privacy the right "to be let alone" and "the right most valued by civilized men." Privacy is often defined negatively -- that is, what it is not. For example, invasion of privacy is seen as interference with an individual's private affairs. Such an invasion can be warranted or unwarranted under law, depending on the purpose, means employed and the nature of the information sought. There is no single, universally accepted definition of privacy. Nor are privacy protections specifically guaranteed by the U.S. Constitution, in contrast to freedom of speech, press, and religion, although the Supreme Court has recognized a Constitutional right of privacy. As detailed in Appendix C, each of the 50 states has had its own set of laws regarding privacy, creating unequal treatment of privacy from jurisdiction to jurisdiction.

The rise of electronic records and the underlying digital and network technologies have put privacy protections in play repeatedly over the years. Consider the chronology of one example from the federal government:

- The Privacy Act of 1974 was passed by Congress to protect the privacy rights of citizens from intrusions by the federal government. The act prohibited the inter agency exchange of personally identifiable information held by government agencies.
- The Paperwork Reduction Act (1980) effectively allowed all personally identifiable information gathered by government to be made available to any agency. Coupled with the proliferation of automated technologies, the Act allowed "computer matching" across databases.
- The 1988 Computer Safeguards Bill was then introduced to again limit the federal government's use of computer records.[53]

As Dr. Cavoukian and her co-author suggest, privacy rights invariably must be balanced against other considerations -- and those considerations may change over time:

> We do not suggest that privacy is an absolute right that reigns supreme over all rights. It does not. However, the case for privacy will depend on a number of factors that can influence the balance -- the level of harm to the individual involved versus the needs of the public.[54]

Given that criteria, there would be a different balance struck for the release of personally identifiable about a convicted sexual predator who has been released into a community than a person in the same community who is HIV-positive. Protecting the identity of the

[53] Anne Branscomb, *Who Owns Information?: From Privacy to Public Access*, New York: 1994.
[54] Ann Cavoukian and Don Tapscott, *Who Knows: Safeguarding your privacy in a networked world*, New York: McGraw-Hill, 1996: 16.

predator may put children in harm's way. Disclosing the name of the HIV-positive individual may lead to loss of employment, benefits and housing.

Judging by public comment received by the Work Group and the media coverage of these issues, the is a growing concern that electronic records are both infinitely changeable and disturbingly durable. The public concern can be fairly summarized as follows:

- If you are alive, you are constantly creating records about yourself. That these records can be gathered, co-mingled and compared can tell others more about you than you ever intended. Those records are also difficult to evade.
- Moving to a new town no longer affords the opportunity to re-create yourself. Before long, your employer, banker and local retailer probably have a pretty good idea of where you have been and what you have been doing. Depending on their resourcefulness, they can probably discover a skeleton or two -- even if it has no bearing on your current life or relationship with them.
- That records can now follow you most everywhere points to the loss of "social forgiveness." Even minor misdeeds can follow otherwise solid citizens for life. In a networked world, there may be nowhere left to exercise your right "to be let alone."

V. Digital Records: Pendulum Swinging Back.

In her testimony before the Work Group, Dr. Cavoukian commented on the impact of digital technology on personally identifiable information and the growing concern in the public about how information about individuals is handled in both the public and private sectors.

She said the recent Lexis-Nexis P-TRAK controversy was an illustrative example of "driftnet data fishing," highlighting the impact of digital technology on records stewardship. In a paper-based world, records were discrete and had to be compared and compiled by hand in a difficult and time-consuming process. However, the emerging digital environment lends itself to the ready co-mingling of once discrete records.

Dr. Cavoukian said the short answer to the question before the Work Group was that one cannot provide absolute safeguards for personally identifiable information when public records are released for commercial purposes. However, the long answer was that there were a number of steps that can be taken -- voluntary privacy codes, physical and computer security provisions, and the redaction of personally identifiable information -- to provide some safeguards for citizens and their personal information. If those steps are taken, it is possible to re-introduce at least some level of "social forgiveness."

Before a decades-long automation process began in government, paper searches provided a form of protection because of the effort required to find the information. It was a cumbersome process that discouraged all but the most motivated requester. The gathering of personally identifiable information in searchable databases creates risks today

that did not exist before. After years of focusing on the automation process, the pendulum appears to be swinging back to consider the combined effects of all such technological advances on personal privacy. It is not that the public is relaxing its demands on government for efficiency and responsive service delivery. More to the point is that the public expects the benefits of those efficiencies without compromising their personally identifiable information.

VI. Prospects for Self Correction.

The Work Group was asked by the Governor to address safeguards for personally identifiable information when public records are released for business or commercial purposes. As will be discussed below, there are measures that government can take to protect personal information provided by citizens.

Everyone exchanges information for other information and benefits every day. Much has been written elsewhere about what citizens can do for themselves to restrict the circulation of personal information about them. The Work Group concurs with the major theme that runs through this material -- that individuals consider the privacy implications of engaging in day-to-day transactions in the marketplace.

There is no single solution to the vexing privacy challenges inherent in a digital, networked environment. Personal responsibility and proper government stewardship must be matched by meaningful privacy protections by the private sector if personally identifiable information is to be safeguarded when public records are released for commercial purposes.

It is difficult to overstate the importance of safeguards in the private sector. Given the massive volumes of information it accumulates, compounded by ever increasing capabilities to co-mingle once discrete databases, the private sector is probably more important in terms of its impact on privacy than the governments from which it acquires information.

Government's increasing reliance on public-private partnerships and privatization has raised concerns in some circles about data integrity and personal privacy. In fact, as discussed below, legislative and contractual are in place, although they vary from agency to agency -- and program to program.

There is a strong case to be made for the competitive advantages of privacy protections in the private sector. Privacy advocates see this model as one way to help ensure the legal and authorized use of public records. Government could impose the same threshold for handling confidential records in the private sector as exists in the public sector -- an oath of secrecy or contractual obligations to comply with privacy code in order to have continued access to the records. Representatives from R.L. Polk and Commercial Information Systems (CIS) have told the Work Group that they have voluntarily imposed these kinds of restrictions on themselves.

Those that advocate the idea that there are competitive advantages derived through privacy protections in the private sector recognize that:

> [S]ome business needs legitimately require the collection of personal information. But the two goals of needing information for legitimate business purposes and privacy protection need not be mutually exclusive. Instead of competing against each other, the two can join forces if privacy-protective practices are built into one's business. In these times of fiercely competitive markets, if protecting consumer privacy is viewed as a component of good business practice, then privacy need not be treated as an adversary -- it can be made an ally. When a company designs its products and services with privacy in mind, it also enhances the security of its information holdings, which in turn enhances customer confidence. That trust has considerable value.[55]

While this approach may seem counter intuitive initially, it may be the basis of a self correcting process over time. Dr. Cavoukian cautions that any self correcting process will require external intervention to act as a catalyst to begin the necessary behavioral change. She said the private sector must be given a "nudge" to move in the right direction. Those "nudges" must come from a combination of public pressure and governmental direction.

Work Group members said the prospect of eventual self correction should not prevent government from taking timely action to mitigate against possible harm to personal privacy.

[55] Ibid: 185.

VII. Spanning the Gap: Government Action.

Public comment before the Work Group reflected, in part, the hope that government can be trusted to protect personally identifiable information. In this respect, government must act as a barometer for public sentiment and concern.

1. Government Responsibility

Government often holds the unique authoritative record on matters of public concern -- and intense personal consequence. The Work Group believes government must show leadership in safeguarding personal privacy. The rapid increases in unauthorized access to personally identifiable information via the Internet has prompted some to question the utility of limiting the circulation of such information from only one of many sources. However, when that single source is government, there are compelling reasons to provide safeguards:

- *Public Trust:* The Work Group believes that digital stewardship is foundational to the preservation of public trust and confidence in government. The Work Group also recognizes that open government is a necessary pre-condition for public trust.
- *Public Benefit:* The Work Group has already explained its rationale for believing that the greatest public benefit is realized when public records are used within their "original orbit." Any public records released for commercial purposes should be limited to targeted use within their original orbit -- that is, the purpose for which they were collected. General or secondary use of records should be restricted.
- *Data Integrity:* Privacy protections are likely to encourage individuals to provide more complete, current and -- by extension -- accurate information.

2. Government Action

a. Legislation

The Work Group is considering a proposal that would request the necessary legislative changes to allow the "salting" of lists of individuals in order to identify abuse under the Open Records Act. Under current law, there are no penalties for agencies that improperly provide the list. There are no penalties if a company misrepresents how it will use the list of if it passes it on to a second party that uses the information to contact people on the list.

A white paper developed for the Work Group explained that businesses would be warned up front of possible penalties and the fact they could be sued for damages. The threat of loss of access to records would likely prove to be the greatest disincentive to commercial interests. In addition, the white paper suggested the introduction of financial disincentives for abuse, such as assessing a penalty on a per name basis for each violation. As envisioned, the state would charge a penalty on a per name bases for each violation. The potential for creating a financial disincentive is considerable given the size of the

databases involved. Some databases contain thousands of names -- other databases hold names that number in the millions.

The Work Group has also discussed the relative merits of revisiting the definitions in statute. There has been discussion about differentiating between public and private information in government records. There has also been discussion of creating a legal distinction between commercial and business use.

Finally, the Work Group's deliberations are coincident with at least three other activities in state government that touch on privacy issues:

- The Department of Licensing is requesting legislation to reconcile state law with provisions of the federal Driver's Identity Protection Act.
- There is a legislative proposal related to background checks provided through the Washington State Patrol.
- The Department of Licensing and the Washington State Patrol were directed by the Governor to "conduct a study regarding the feasibility and privacy implications of providing drivers license data to private entities."[56] The Governor has also asked that the study be delayed so information by the present Work Group could be taken into consideration.

b. Contractual Limitations

Agencies enter into contractual agreements with authorized commercial interests that define permissible use and prescribe penalties for abuse. The sanctions are often cast in terms of loss of access to the data. As a matter of practice, commercial interests salt lists in their possession to ensure their customers are using the information in ways that are consistent with their contracts.

The larger information and marketing industries have responded to recent revelations about privacy breeches with increased reliance on independent audits and the introduction of voluntary privacy codes.

The Work Group believes there may be merit in providing for both salting of lists of individuals and compliance audits in structuring contracts between public entities and private sector information vendors.

c. System Design

The difficulties and prohibitive costs associated with retrofitting existing computer systems with the capability to mask (or redact) personally identifiable information point to the need to build privacy into system design at the ground floor. Governments and their private partners in commercial release should build privacy into all programs and systems

[56] ESHB 2343 (Full Veto)

at the design stage. An assessment of the cost of privacy provisions should be part of the decision package for new systems.

Washington state is by no means alone in its efforts to find privacy-friendly solutions in its handling of personally identifiable information. As a significant purchaser of information technology, government may be in a position to influence design decisions by vendors --making it clear that it will only by those systems that safeguard privacy through the redaction of personally identifiable information or some other means.

VIII. Conclusion.

In answering the question, *How can citizens be assured that personal information about them will be safeguarded when public records in electronic format are released for business or commercial purposes?* the Work Group finds:

- privacy policies must seek to balance business' and government's needs for access to information with the individual's expectations of privacy.
- there is no interest in restricting access to information about the performance of public institutions or about public policy
- the government has a duty to safeguard the private lives of ordinary citizens from invasion.
- revelations about high tech privacy breeches are fueling concern among citizens about the handling of their personally identifiable information.
- the public expects government to safeguard their personally identifiable information.
- private sector industry groups have responded to public concern by introducing voluntary codes of practice to protect privacy.
- the rise of electronic records that follow individuals from place to place and over time results in the to the loss of "social forgiveness."
- the provision in Washington's Open Records Act to prohibit access to information "that is highly offensive to a reasonable person and of no legitimate public concern" is a very high threshold to meet in protecting privacy.
- consistent with the code of *Fair Information Practices*, the collection of personal information should be limited to that which is necessary to fulfill legislative mandates of respective agencies.
- any public records released for commercial purposes should be limited to targeted use within their original orbit -- that is, the purpose for which it was collected.
- general or secondary use of records should be restricted.
- after years of focusing on the automation process, the pendulum appears to be swinging back to consider the combined effects of technological advances on personal privacy.
- government, the private sector and individuals all have roles to play in safeguarding personally identifiable information.
- strong privacy protection can be a competitive advantage in the private sector.
- the Work Group is considering legislative provisions to allow --and possibly require -- the salting of lists to detect unauthorized use of lists of individuals.

- contractual obligations with information resellers can increase accountability for unauthorized use.
- loss of access may be a more effective disincentive than monetary penalties alone.
- privacy considerations should be built into new computer system design.

APPENDIX A: OECD FAIR INFORMATION PRACTICES

Based on the Organization for Economic Cooperation and Development (OECD), *Guidelines on the Protection of Privacy and Transport of Flows of Personal Data*, September 23, 1980; and the Council of Europe, *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, January 28, 1981 (Treaty Series 108).

1. *The social justification principle*: The collection of personal data should be for a general purpose and specific uses which are socially acceptable.

2. *The collection limitation principle*: Personal data should be restricted to the minimum necessary to accomplish the purpose of collection, should be obtained by lawful means and with the knowledge of the data subject.

3. *The data quality principle*: Personal data should, for the purposes for which they are to be used, be accurate, complete and up-to-date.

4. *Purpose specification principle*: The purpose for which personal data are collected should be made known to the data subject not later than the time of collection and subsequent use should be limited to those purposes. For example, there is often a statement at the bottom of contest entry forms notifying the entrant that the personal information on the entry form may be used for marketing purposes. However, if the individual is applying for a bank account, personal loan or even a driver's license, this approach becomes coercive because of the imbalance of power between the individual and the organization collecting the data.

5. *Use limitation principle*: Personal data should not be disclosed or made available except with the consent of the data subject, the authority of law or routine practice.

6. *Security safeguards principle*: Personal data should be protected by safeguards which are reasonable and appropriate to prevent loss, destruction, modification or disclosure of the data.

7. *The openness principle*: There should be a general policy of openness about developments, practices, and policies with respect to personal data.

8. *Individual participation principle*: An individual should have the right to confirm the existence of data, to examine the data, to correct and update the data and to be informed of reasons if access to data is denied.

9. *Time limitation principle*: Personal data, once the purposes of use have expired, should be destroyed, archived or de-identified.

10. *The accountability principle*: There should be, in respect of any personal data record, an identifiable data controller.(46)

APPENDIX B: CSA PRINCIPLES IN SUMMARY

Canadian Standards Association (CSA) Draft Model Code for the Protection of Personal Information

1. Accountability. An organization is responsible for personal information under its control and shall designate a person who is accountable for the organization s compliance with the following principles.

2. Identifying Purposes. The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. Consent. The knowledge and consent of the individual are required for the collection, use or disclosure of personal information except where inappropriate.

4. Limiting Collection. The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. Limiting Use, Disclosure and Retention. Personal information shall not be used or disclosed for purposes other than those for which it was collected except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

6. Accuracy. Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards. Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness. An organization shall make readily available to individuals specific information about its policies and practices relating to its handling of personal information.

9. Individual Access. Upon request, an individual shall be informed of the existence, use and disclosure of personal information about the individual and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance. An individual shall be able to challenge compliance with the above principles with the person who is accountable within the organization.

APPENDIX C: STATE PRIVACY LAWS

Excerpted from *Citizen Access to Local Government Infostructure: A Guide for Public Policy Makers*, the National League of Cities and the State Municipal League Advisory Group.

State	Statute
Alaska	• 44.99.300 Fair information Practices law creates a process for citizen to challenge the accuracy of personal information subject to public disclosure. • Agencies must notify data subject of: • 1. law permitting information • 2. consequences of not providing information • 3. anticipated use and disclosure of the data • 4. how to challenge the accuracy
California	• Civil Code Sec. 1798 Fair Information Practices Act gives citizens right to see and correct state files about themselves. State agencies may disclose personal information only in limited circumstances. • Law permits invasion-of-privacy lawsuits against a person who intentionally discloses personal information that was known to come from a state or federal agency in violation of law. • Motor vehicle registration information may be sold at cost, but buyer must identify the reason for the request. • Data is freely available to press and an attorney, but there is a ten-day wait for person requesting access to another person's motor vehicle records.
Colorado	• 24-27-204 Individuals are permitted to examine their own records, but state must keep following records confidential: medical and personnel files, library material; address and telephone number of public school students.
Connecticut	• 4-190 State and local Government are to maintain only necessary information and provide individual access to such information. Agencies must keep a record of disclosures.
Florida	• 282.318 State departments must have information security manager to assure that security procedures for data processing are followed.
Hawaii	• 92F Uniform Information Practices Act permits individuals to have access to "personal records" about themselves. Privacy interests must be balanced against public interest in disclosure of medical, social service, financial and performance evaluation data. Individuals may correct errors. • Office of Information practices within the Department of the Attorney General enforces the law.
Illinois	• 116.43.5 Most state records are public, others may be disclosed if the requester signs an affidavit "that the information shall not be made available to other persons." • Public records law includes language: "Nothing in this section shall require the Secretary of State to invade or assist in the invasion of any person's right to privacy."

Indiana

- 4-1-6 Fair Information Practices Act requires that state agencies may determine when personal information may be exchanged
- Citizen has a right to inspect personal information except medical records; however, agencies define whether personal data is confidential or public.

Kentucky

- 61.870 State open records law mandates access to any and all records of public agencies except records of personal nature, certain law enforcement records and a few other categories.
- Provision is made that persons shall have access to public records relating to them.

Maine

- 5.1851 Bureau of Central Computer Services established to effect consolidation of data processing equipment and to safeguard confidentiality of information files

Massachusetts

- 66A Agency must designate individual responsible for personal data systems and must enact regulation governing outside access and individual challenge and correction
- Each personal data system must be registered with the secretary of state.

Minnesota

- 13.01 Data Practices Act covers state agencies and institutions, school boards, local commissions but not townships. Defines confidential personal data not available to the individual. Each agency must designate a person to be responsible for data banks and report annually to state department of administration.
- Individual must be told purpose and use of information and has a right to contest personal information before action taken against them due to "Computer matching"

Mississippi

- 25-53-55 If "confidential information" is wrongfully released to a state agency, the person may complain to the central data processing authority and charges may be brought against employee involved.

New Hampshire

- 7-A Information Practices Act requires data banks Maintained by state agencies to be registered with the state department of administration.

New York

- 91 "each agency maintaining a system of records shall prepare a notice describing each of its systems of records," including the uses made of each category of records and the disclosures of personal information that the agency regularly makes.
- The Committee on Public Access to Records is responsible for registering all state agency data banks, to take citizen complaints, and to issue advisory opinions.
- Citizens have a right to see and correct their own files.

Ohio

- 1346.01 Notice stating the nature and character of any personal information system and name of individual directly responsible for it must be filed with the director of administrative services. Agencies maintaining theses systems must inform persons whether the information they are asked to provide is legally required and must collect only personal information necessary and relevant to the functions of that agency.
- With certain specific exemptions, personal information may not be disclosed without the consent of the individual. The law provides for accessing, challenging and amending one's own record

Oklahoma

- 74.118.17 Data Processing Planning and Management Act provides for storage of confidential data in centralized data processing center to preclude access without authorization

Utah

- 63-2-103 Government Records Access and Management Act includes principles of fair information practices found in federal privacy act.
- Types of data collected by state agencies are reported annually. There four categories of personal information: public, private, confidential, and protected.
- Individually have the right to contest the accuracy of their own data.

Virginia

- 2.1-377 Privacy Protection Act of 1976 prohibits secret personal information systems and collection of unneeded, inappropriate, inaccurate information.
- Law provides for access and correction.

Washington

- 43.105.040 (4) Governor, after consultation with data processing advisory committee, has power to set policy for data processing, including standards to establish and maintain the confidential nature of information.

Wisconsin

- Ch.19 Seven-person Privacy Council appoints a privacy advocate to present the privacy perspective instate policy making and to assist citizens in access to their own files.
- State agencies must register their records and develop rules of conduct for handling of personal data.
- Individual must be notified before adverse action is taken as result of computer matching unless the state or local agency finds the information used "sufficiently reliable."